UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/759,627	01/12/2001	Ryan J. Nobrega	3399P040	2387

7590 10/10/2006

Jordan M. Becker
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Seventh Floor
12400 Wilshire Boulevard
Los Angeles, CA 90025-1026

EXAMINER	
LIVERSEDGE, JENNIFER L	
ART UNIT	**PAPER NUMBER**
3692	

DATE MAILED: 10/10/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/759,627	NOBREGA ET AL.	
	Examiner	Art Unit	
	Jennifer Liversedge	3628	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *21 July 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *17-45 and 50-56* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *17-45 and 50-56* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Amendment

This Office Action is responsive to Applicant's amendment and request for reconsideration of application 09/759,627 filed July 21, 2006.

The amendment contains original claims: 18-23, 25-40, 42-45 and 51-56.

The amendment contains previously presented claims: 41.

The amendment contains amended claims: 17, 24 and 50.

Claims 1-16 and 46-49have been canceled.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 17-21, 24-26, 29-35, 41-45, 50-53 and 55-56 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,609,113 B1 to O'Leary et al. (further referred to as O'Leary).

Regarding claim 17, O'Leary discloses a method of facilitating a credit card transaction (column 5, lines 42 – 46) between a consumer using a wireless

communication device (column 8, line 63 – column 9, line 4 and column 9, lines 17 – 20) and a provider of a product or service (column 7, lines 16 – 23), the method comprising:

In a commerce platform implemented as one or more computer systems operated by a single business entity (column 9, lines 26-28; column 10, line 65 – column 11, line 3; column 26, lines 25-59),

storing personal information of the consumer, including a credit card number of a credit card issued to the consumer (column 9 line 65 – column 10, line 10);

receiving information for requesting the transaction from a remote entity (column 15, line 66 – column 16, line 1);

sending information on the transaction to the wireless communication device (column 16, lines 5 – 7);

receiving a signal from the wireless communication device indicating acceptance of the transaction (column 16, lines 6 – 17);

receiving a personal identification code from the wireless communication device (column 9, lines 49-52; column 11, lines 4-15 and 38-41; column 15, lines 33 – 39);

using the received personal identification code and the stored personal information on the consumer to verify the identity of the consumer (column 11, lines 4 – 15 and 38-41 and column 15, lines 33 – 39; column 19, lines 18-21), and

in response to verifying the identity of the consumer, sending to a remote entity other than said single business entity a transaction request including information on the transaction and the credit card number (column 5, lines 42-50; column 10, lines 17 –

35), for initiation of a transaction approval process (column 10, lines 23 – 30 and column 16, lines 18 – 32).

Regarding claim 24, O' Leary discloses a method of facilitating a credit card transaction (column 5, lines 42 – 46) between a consumer using a wireless communication device (column 8, line 63 – column 9, line 4 and column 9, lines 17 – 20) and a provider of a product or service (column 7, lines 16 – 23), the method comprising:

In a commerce platform implemented as one or more computer systems operated by a single business entity (column 9, lines 26-28; column 10, line 65 – column 11, line 3; column 26, lines 25-59),

storing personal information of the consumer in a database within a trusted domain (column 4, lines 54 – 58 and column 9 line 65 – column 10, line 10), the trusted domain excluding the provider (column 5, lines 57-60; column 7, lines 8 – 12 and lines 43 – 47), the personal information including a credit card number of a credit card issued to the consumer (column 9 line 65 – column 10, line 10).

O'Leary further discloses wherein consumers can be excluded from access to the database (column 10, lines 42 – 47). The practice of excluding individuals from access to a database is well known to those of ordinary skill in the art. The motivation is to prevent certain or all individuals from gaining access to the information stored within the database in order to maintain the integrity and confidentiality of the data therein.

receiving information for requesting the transaction from a remote entity (column 15, line 66 – column 16, line 1), the information for requesting the transaction including an amount of the transaction and a provider identifier (column 16, lines 1 – 5);

storing the information for requesting the transaction (column 11, lines 4 – 25);

sending information on the transaction (column 15, line 66 – column 16, line 7) to the wireless communication device via a wireless network (column 8, line 63 – column 9, line 4 and column 9, lines 17 – 20);

receiving a signal from the wireless communication device indicating acceptance of the transaction by the consumer (column 16, lines 6 – 17);

receiving a personal identification code from the wireless communication device via the wireless communications network (column 9, lines 49-52; column 11, lines 4-15 and 38-41; column 15, lines 33 – 39);

using the received personal identification code and the stored personal information on the consumer to verify the identity of the consumer (column 11, lines 4 – 15 and 38-41; column 15, lines 33 – 39; column 19, lines 18-21), and

in response to verifying the identity of the consumer, sending to a remote entity other than said single business entity a transaction request including information on the transaction and the credit card number (column 5, lines 42-50; column 10, lines 17 – 35), for initiation of a transaction approval process (column 10, lines 23 – 30 and column 16, lines 18 – 32), wherein the credit card information of the consumer is not permitted to pass outside the trusted domain (column 5, lines 57 – 60, column 7, lines 8-12 and lines 42 – 46);

receiving a signal indicating the transaction has been approved (column 16, lines 35 – 38); and

in response to receiving the signal indicating the transaction has been approved,

storing a digital receipt of the transaction (column 5, lines 8 – 12 and lines 23 – 25; column 9, line 65 – column 10, line 9 and column 10, lines 21 – 33), and

sending a signal to the wireless communication device over the wireless communication network to cause the wireless communication device to output a message confirming completion of the transaction (column 10, lines 21 – 35).

Regarding claim 33, O'Leary discloses a method of facilitating a credit card transaction (column 5, lines 42 – 46) between a consumer and a provider of a product or service (column 7, lines 16 – 23), the method comprising:

receiving information associated with the transaction from a remote terminal operated by the provider (column 11, lines 4 – 25 and column 15, line 66 – column 16, line 1);

determining whether the transaction is of a predetermined type (column 10, lines 16 – 21);

if the transaction is determined not to be of the predetermined type, then initiating a transaction approval process by transmitting at least a portion of the received information to a clearing network for approval of the transaction (column 5, lines 42-50; column 7, lines 3-7; column 10, lines 21-35);

if the transaction is determined to be of the predetermined type, then transmitting the received information to a remote validation entity other than the clearing network over a secure channel (column 4, lines 54 – 65), to enable validation of the transaction by the remote validation entity (column 5, lines 51-60; column 10, lines 21-35), and

upon receiving an indication that the transaction has been validated by the remote validation entity, initiating a transaction approval process by transmitting at least a portion of the information to the clearing network for approval of the transaction (column 7, lines 8-23; column 10, lines 21-35).

Regarding claim 41, O'Leary discloses a method of facilitating a credit card transaction (column 5, lines 42 – 46) between a consumer using a wireless communication device (column 8, line 63 – column 9, line 4 and column 9, lines 17 – 20) and a provider of a product or service (column 7, lines 16 – 23), the method comprising:

providing a computer-implemented portal, through which the consumer can remotely access a commerce application (column 4, lines 59 – 62 and column 6, lines 27 – 52);

storing personal information of the consumer in a database within a trusted domain (column 4, lines 54 – 58 and column 9 line 65 – column 10, line 10), the trusted domain excluding the provider (column 5, lines 57-60; column 7, lines 11 – 12 and lines 43 – 47) the personal information including a credit card number of a credit card issued to the consumer (column 4, lines 54 – 58 and column 9 line 65 – column 10, line 10).

O'Leary further discloses wherein consumers can be excluded from access to the database (column 10, lines 42 – 47). The practice of excluding individuals from access to a database is well known to those of ordinary skill in the art. The motivation is to prevent certain or all individuals from gaining access to the information stored within the database in order to maintain the integrity and confidentiality of the data therein.

receiving, from a remote entity within the trusted domain, information for requesting the transaction (column 15, line 66 – column 16, line 1), including an amount of the transaction and a provider identifier (column 16, lines 1 – 5);

storing the information for requesting the transaction (column 11, lines 4 – 25);

generating a session identifier corresponding to the transaction in response to receiving the information for requesting the transaction (column 11, lines 4 – 25 and column 12, lines 59 – 63; column 16, lines 13-17);

associating the session identifier with the stored information for requesting the transaction (column 11, lines 4 – 25 and column 15, line 66 – column 16, line 5; column 16, lines 13-17);

sending the session identifier to a remote entity, for subsequent communication to the consumer (column 11, lines 4 – 25 and column 15, line 66 – column 16, line 5; column 16, lines 13-17);

receiving a confidential personal identification code and a user-input session identifier from a wireless communication device via a communications network (column 11, lines 4 – 25; column 16, lines 13-17);

using the received personal identification code, the user-input session identifier, and the stored personal information of the consumer to attempt to validate the transaction (column 15, line 66 – column 16, line 5; column 16, lines 13-17), including

using the personal identification code and the stored personal information to verify the identity of the consumer (column 15, lines 33 – 39 and lines 54 – 57; column 15, line 66 – column 16, line 5; column 16, lines 13-17), and

using the user-input session identifier to look up the stored information for requesting the transaction and to associate the consumer with the transaction (column 11, lines 4 – 25; column 16, lines 13-17);

if the transaction is successfully validated, then sending information on the transaction (column 15, line 66 – column 16, line 1) to the wireless communication device over the wireless network (column 8, line 63 – column 9, line 4 and column 9, lines 17 – 20) to cause the wireless communication device to output a prompt to accept or decline the transaction (column 16, lines 5 – 11);

receiving a signal from the wireless communication device indicating acceptance of the transaction (column 16, lines 5 – 11);

in response to receiving the signal indicating acceptance of the transaction, sending to a remote entity a transaction request including information on the transaction and the credit card number (column 10, lines 17 – 21 and column 16 lines 18 – 22), for initiation of a transaction approval process by a clearing network (column 10, lines 23 – 30 and column 16, lines 18 – 32), without sending the credit card information outside the trusted domain (column 5, lines 57 – 60; column 7, lines 8 – 12 and lines 42 – 46);

receiving a signal indicating the transaction has been approved by the clearing network (column 16, lines 28 – 38); and

in response to receiving the signal indicating the transaction has been approved by the clearing network,

storing a digital receipt of the transaction in association with the identity of the consumer (column 5, lines 8 – 12 and lines 23 – 25; column 9, line 65 – column 10, line 9 and column 10, lines 21 – 33); and

sending a signal to the wireless communication device over the wireless communication network to cause the wireless communication device to output a message confirming completion of the transaction (column 10, lines 21 – 35).

Regarding claim 50, O'Leary discloses a processing system to facilitate a credit card transaction (column 5, lines 42 – 46) between a plurality of consumers using a wireless communication device (column 8, line 63 – column 9, line 4 and column 9, lines 17 – 20) and a plurality of providers of products or services (column 7, lines 16 – 23), the processing system comprising:

a database of personal information of the consumers, including, for each of the consumers, a credit card number of a credit card issued to a consumer (column 4, lines 54 – 58 and column 9 line 65 – column 10, line 10);

a processor (page 4, lines 54 – 55); and

a memory containing instructions for execution by the processor (column 10, lines 14 – 34) to control the processing system to receive information for requesting the transaction from a remote entity (column 15, line 66 – column 16, line 1);

send information on the transaction (column 15, line 66 – column 16, line 7) to one of the wireless communication devices (column 8, line 63 – column 9, line 4 and column 9, lines 17 – 20);

receive a signal from the wireless communication device indicating acceptance of the transaction (column 16, lines 6 – 17);

receive a personal identification code from the wireless communication device (column 9, lines 49-52; column 11, lines 4-15 and lines 38-41; column 15, lines 33 – 39);

use the received personal identification code and the stored personal information on the consumer to verify the identity of the consumer (column 11, lines 4-15 and 38-41; column 15, lines 33-39; column 19, lines 18-21), and

in response to verifying the identity of the consumer, send to a remote entity a transaction request including information on the transaction and the credit card number (column 5, lines 42-50; column 10, lines 17-35), for initiation of a transaction approval process (column 10, lines 23 – 30 and column 16, lines 18 – 32).

Regarding claims 18 and 51, O'Leary discloses a method and processing system wherein storing personal information of the consumer comprises storing personal information of the consumer in a database within a trusted domain (column 4, lines 54 –

58 and column 9 line 65 – column 10, line 10) the trusted domain excluding the provider (column 5, lines 57 – 60; column 7, lines 8 – 12 and lines 43 – 47).

O'Leary further discloses wherein consumers can be excluded from access to the database (column 10, lines 42 – 47). The practice of excluding individuals from access to a database is well known to those of ordinary skill in the art. The motivation is to prevent certain or all individuals from gaining access to the information stored within the database in order to maintain the integrity and confidentiality of the data therein.

Regarding claims 19, 25, 42 and 52, O'Leary discloses a method and processing system wherein the stored personal information of the consumer is not permitted to pass outside the trusted domain at any time during performance of the method (column 5, lines 57 – 60; column 7, lines 8 – 12 and lines 42 – 46).

Regarding claims 20 and 56, O'Leary discloses a method and processing system further comprising:

receiving a signal indicating the transaction has been approved (column 16, lines 35 – 38); and

in response to receiving the signal indicating the transaction has been approved, storing a digital receipt of the transaction (column 5, lines 8 – 12 and lines 23 – 25; column 9, line 65 – column 10, line 9 and column 10, lines 21 – 33), and

sending a signal to the wireless communication device to cause the wireless communication device to output a message confirming completion of the transaction (column 10, lines 21 – 35).

Regarding claims 21 and 26, O'Leary discloses a method further comprising providing telecommunications services (column 4, lines 38 – 45) to users of a plurality of wireless communications devices on a wireless communications network (column 8, line 63 – column 9, line 4 and column 9, lines 17 – 20), including storing user account information (column 4, lines 54 – 58 and column 9 line 65 – column 10, line 1) for each of the plurality of users, including a consumer (column 9, lines 17 – 23 and column 15, lines 33 – 39).

Regarding claim 29, O'Leary discloses a method wherein a remote entity is within the trusted domain, and wherein receiving information for requesting the transaction comprises receiving the information from the remote entity via a secure channel (column 4, lines 54 – 65).

Regarding claims 30 and 44, O'Leary discloses a method wherein the stored digital receipt is remotely accessible to the consumer (column 9, lines 17 – 23; column 11, lines 23 – 25 and column 18, lines 47 – 51).

Regarding claims 31 and 55, O'Leary discloses a method and processing system providing a computer-implemented portal, through which the consumer can remotely access a commerce application (column 4, lines 59 – 62 and column 6, lines 27 – 52).

Regarding claims 32 and 45, O'Leary discloses a method wherein the stored digital receipt is remotely accessible to the consumer via the portal (column 6, lines 27 – 52).

Regarding claim 34, O'Leary discloses a method wherein the information received from the remote terminal does not include a credit card number if the transaction is of the predetermined type, such that the information transmitted to the remote validation entity does not include a credit card number, and such that the remote validation entity validates the transaction without requiring the consumer or the provider to communicate a credit card number in connection with the transaction (column 5, lines 51-60; column 7, lines 8-23; column 10, lines 14-35).

Regarding claim 35, O'Leary discloses a method wherein the information received from the remote terminal includes a credit card number if the transaction is not of the predetermined type (column 5, lines 42 – 50; column 7, lines 3-7; column 10, lines 14-35).

Regarding claim 43, O'Leary discloses a method wherein receiving information for requesting the transaction comprises receiving the information from the remote entity via a secure channel (column 4, lines 54 – 65).

Regarding claim 53, O'Leary discloses a processing system wherein the processing system is operated by a telecommunications carrier (column 4, lines 38 – 45) providing wireless communications services (column 8, line 63 – column 9, line 4 and column 9, lines 17 – 20) to the plurality of consumers (column 9, lines 17 – 23 and column 15, lines 33 – 39).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* **v.** *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claims 22 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over O'Leary as applied to claims 21 and 24 above, and further in view of WO 96/13814 to Vazvan (further referred to as Vazvan).

Regarding claims 22 and 27, O'Leary does not disclose a method further comprising, prior to sending information on the transaction to the wireless communication device receiving a unique identifier of the wireless communication device from a remote entity; and identifying the wireless communication device and an associated user account based on the unique identifier.

However, Vazvan discloses a method further comprising, prior to sending information on the transaction to the wireless communication device receiving a unique identifier of the wireless communication device from a remote entity; and identifying the wireless communication device and an associated user account based on the unique identifier (pages 2-3).

It would be obvious to one of ordinary skill in the art at the time of the invention to modify the use of wireless communication devices for payments as disclosed by O'Leary to adapt the use of unique identifiers received from remote entities for identifying the user as disclosed by Vazvan. The motivation would be to create a secure system in which a unique identifier is used to identify the device being used for a transaction of payment such that added layers of security exist against fraud and to provide an efficient means by which to associate a device with a user to authorize transactions.

Claims 23, 28 and 39-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over O'Leary and Vazvan, and further in view of U.S. Patent No. 6,868,391 B1 to Hultgren (further referred to as Hultgren).

Regarding claims 23 and 28, neither O'Leary nor Vazvan disclose a method further comprising verifying that the wireless communication device is in geographic proximity to the provider. However, Hultgren discloses a method further comprising verifying that the wireless communication device is in geographic proximity to the provider (column 2, lines 14-21). It would be obvious to one of ordinary skill in the art at the time of the invention to modify the use of wireless communication devices for payments as disclosed by O'Leary and Vazvan to adapt the requirement of geographic proximity to a merchant as disclosed by Hultgren. The motivation would be to perform a security check that the user of the mobile device is at a merchant in order to reduce fraud associated with transactions from unauthorized users and /or users in unauthorized locations.

Regarding claim 39, O'Leary discloses a method of a telecommunications carrier (column 4, lines 38 – 45) facilitating a credit card transaction (column 5, lines 42 – 46) between a consumer using a wireless communication device (column 8, line 63 – column 9, line 4 and column 9, lines 17 – 20) and a provider of a product or service (column 7, lines 16 – 23), the method comprising:

providing telecommunications services (column 4, lines 38 – 45) to users of a plurality of wireless communications devices on a wireless communications network (column 8, line 63 – column 9, line 4 and column 9, lines 17 – 20), including storing user account information (column 4, lines 54 – 58 and column 9 line 65 – column 10, line 1) for each of the plurality of users, the plurality of users including a consumer (column 9, lines 17 – 23 and column 15, lines 33 – 39);

storing personal information of the consumer in a database within a trusted domain (column 4, lines 54 – 58 and column 9 line 65 – column 10, line 1), the trusted domain excluding the provider (column 7, lines 11 – 12 and lines 43 – 46), the personal information including a credit card number of a credit card issued to the consumer (column 4, lines 54 – 58 and column 9 line 65 – column 10, line 1);.

O'Leary further discloses wherein consumers can be excluded from access to the database (column 10, lines 42 – 47). The practice of excluding individuals from access to a database is well known to those of ordinary skill in the art. The motivation is to prevent certain or all individuals from gaining access to the information stored within the database in order to maintain the integrity and confidentiality of the data therein.

receiving information for requesting the transaction from a remote entity (column 15, line 66 – column 16, line 1), the information for requesting the transaction including an amount of the transaction, and a provider identifier (column 16, lines 1 – 5);

storing the information for requesting the transaction (column 11, lines 4 – 25);

identifying the wireless communication device and an associated user account based on the unique identifier (column 9, lines 49 – 52 and column 15, lines 32 – 39 and lines 54 – 57);

sending information on the transaction (column 15, line 66 – column 16, line 1) to the wireless communication device via a wireless network (column 8, line 63 – column 9, line 4 and column 9, lines 17 – 20);

receiving a signal from the wireless communication device indicating acceptance of the transaction by the consumer (column 16, lines 6 – 11);

receiving a personal identification code from the wireless communication device via the wireless communications network (column 15, lines 33 – 39);

using the received personal identification code and the stored personal information on the consumer to verify the identity of the consumer (column 11, lines 4 – 15 and column 15, lines 33 – 39), and

if the identity of the consumer is verified, sending to a remote entity a transaction request including information on the transaction and the credit card number (column 10, lines 17 – 21 and column 16 lines 18 – 22), for initiation of a transaction approval process (column 10, lines 23 – 30 and column 16, lines 18 – 32), wherein the credit card information of the consumer is not permitted to pass outside the trusted domain (column 5, lines 57 – 60, column 7, lines 42 – 46);

receiving a signal indicating the transaction has been approved (column 16, lines 35 – 38); and

in response to receiving the signal indicating the transaction has been approved,

storing a digital receipt of the transaction (column 5, lines 8 – 12 and lines 23 – 25; column 9, line 65 – column 10, line 9 and column 10, lines 21 – 33), and

sending a signal to the wireless communication device over the wireless communication network to cause the wireless communication device to output a message confirming completion of the transaction (column 10, lines 21 – 35).

O'Leary does not disclose information from a remote entity including a unique identifier of the wireless communications device. However, Vazvan discloses information from a remote entity including a unique identifier of the wireless communication device (pages 2-3). It would be obvious to one of ordinary skill in the art at the time of the invention to modify the use of wireless communication devices for payments as disclosed by O'Leary to adapt the use of unique identifiers received from remote entities for identifying the user as disclosed by Vazvan. The motivation would be to create a secure system in which a unique identifier is used to identify the device being used for a transaction of payment such that added layers of security exist against fraud and to provide an efficient means by which to associate a device with a user to authorize transactions.

Neither O'Leary nor Vazvan disclose the method verifying that the wireless communications device is in geographic proximity to the provider. However, Hultgren discloses the method verifying that the wireless communication device is in geographic proximity to the provider (column 2, lines 14-21). It would be obvious to one of ordinary skill in the art at the time of the invention to modify the use of wireless communication devices for payments as disclosed by O'Leary and Vazvan to adapt the requirement of

geographic proximity to a merchant as disclosed by Hultgren. The motivation would be to perform a security check that the user of the mobile device is at a merchant in order to reduce fraud associated with transactions from unauthorized users and /or users in unauthorized locations.

Regarding claim 40, O'Leary discloses a method wherein the stored personal information of the consumer is not permitted to pass outside the trusted domain at any time during performance of the method (column 5, lines 57 – 60; column 7, lines 8 – 12 and lines 42 – 46).

Claims 36-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over O'Leary as applied to claim 33 above, and further in view of U.S. Patent No. 6,188,994 B1 to Egendorf (further referred to as Egendorf).

Regarding claim 36, O'Leary does not disclose a method wherein determining whether the transaction is of a predetermined type comprises determining whether the transaction is of the predetermined type based on the information received from the remote terminal. However, Egendorf discloses a method wherein determining whether the transaction is of a predetermined type comprises determining whether the transaction is of the predetermined type based on the information received from the remote terminal (column 2, lines 31-39; column 3, lines 44-64; column 5, lines 2-12; column 6, line 30 – column 7, line 3). It would be obvious to one of ordinary skill in the

art to modify the use of wireless communication devices for payments as disclosed by O'Leary to adapt the use of transaction determination based on information received from the remote terminal as disclosed by Egendorf. The motivation would be that as the transaction is initiated by the vendor (remote terminal) and that relevant information is being sent as captured by the vendor, to include an indication of the transaction type within the message from the vendor.

Regarding claim 37, O'Leary does not disclose a method wherein determining whether the transaction is of a predetermined type comprises determining whether the received information includes a predetermined code. However, Egendorf discloses a method wherein determining whether the transaction is of a predetermined type comprises determining whether the received information includes a predetermined code (column 2, lines 31-39; column 5, lines 20-32; column 6, lines 30-49; column 6, line 30 – column 7, line 3). It would be obvious to one of ordinary skill in the art to modify the use of wireless communication devices for payments as disclosed by O'Leary to adapt the use of transaction determination based on a code as disclosed by Egendorf. The motivation would be that a code offers a condensed version of the information and would result in quicker transmission, as well as greater security associated with the transaction information, in the transfer.

Regarding claim 38, O'Leary does not disclose a method wherein the information received from the remote terminal may include a credit card number, and wherein

determining whether the transaction is of a predetermined type comprises determining whether the information received from the remote terminal includes a predetermined code in place of a credit card number. However, Egendorf discloses a method wherein the information received from the remote terminal may include a credit card number, and wherein determining whether the transaction is of a predetermined type comprises determining whether the information received from the remote terminal includes a predetermined code in place of a credit card number (column 2, lines 30-67; column 3, lines 44-64; column 6, line 30 – column 7, line 3). It would be obvious to one of ordinary skill in the art to modify the use of wireless communication devices for payments as disclosed by O'Leary to adapt the use of a code in place of a credit card number as disclosed by Egendorf. The motivation would be that a code offers a condensed version of the information and would result in quicker transmission, as well as greater security associated with the transaction information, in the transfer.

Claim 54 is rejected under 35 U.S.C. 103(a) as being unpatentable over O'Leary as applied to claim 50 above, and further in view of U.S. Patent No. 6,868,391 B1 to Hultgren (further referred to as Hultgren).

O'Leary does not disclose a method further comprising verifying that the wireless communication device is in geographic proximity to the provider. However, Hultgren discloses a method further comprising verifying that the wireless communication device is in geographic proximity to the provider (column 2, lines 14-21). It would be obvious to one of ordinary skill in the art at the time of the invention to modify the use of wireless

communication devices for payments as disclosed by O'Leary to adapt the requirement of geographic proximity to a merchant as disclosed by Hultgren. The motivation would be to perform a security check that the user of the mobile device is at a merchant in order to reduce fraud associated with transactions from unauthorized users and /or users in unauthorized locations.

Response to Arguments

Applicant has set forth argument related to the following:

Applicant argues O'Leary does not address the manner in which proximity is used in the present application. This argument is moot based on the new rejection in which Hultgren discloses the requirement of a mobile device being used for a transaction to be within a defined proximity to a merchant in order for the transaction to be conducted.

Applicant argues that O'Leary does not address a session identifier as used in the present application. Applicant has argued that the identifier in O'Leary is a transaction and not a session identifier, in that a session identifier represents several transaction. Applicant further argues that the identifier is not user-input. Examiner argues that O'Leary uses a session identifier in that O'Leary specifically discloses where multiple transactions can be incorporated into one identifier, thus a session identifier. Column 16, lines 13-17 discloses where a number of purchases are made

and then a consolidated payment message is transferred to the wallet. O'Leary further discloses where the identifier is used to designate the transaction for further reference and wherein history or verification can be conducted using the number (column 11, lines 4-14). As the wallet is being used by the user of the account, the user would enter such a number in order to retrieve such information. No one else, besides the user, would have access to the wallet, the passwords required for the wallet, transaction numbers in order to reference such that this information is being input by the user. As way of example, U.S. Patent No. 5,915,022 to Robinson et al. also disclose this feature. Robinson discloses a session identifier and digital receipt which the user inputs in order to check on order status or other account inquiries (column 7, lines 13-15; column 8, lines 29-35 and lines 63-67; column 9, lines 13-15), in which the session identifier consists of multiple transactions within a single session (column 7, lines 1-17).

Applicant argues that the actions as described are not performed by a single business entity operating a platform in O'Leary. However, Examiner points specifically to column 6, line 65 – column 7, line 2 in which a legacy platform is disclosed; to column 9, lines 10-15 in which a central host is disclosed; to column 10, line 65 – column 11, line 3 in which the preferred embodiment is one in which the accounts are maintained at a financial institution or other business such that one business can maintain the accounts and perform the operations; and to column, 10 lines 17-35 in which a single entity, the host of the disclosed system, makes a determination of payment type, approves a purchase, initiates payment through an authorization to a customer's bank

(or the host may be the customer's bank), confirm a the purchase and send a corresponding message and digital receipt showing transaction completion. A single entity maintains a central database of consumers and related consumer information; a single entity performs the operations of an electronic method for making purchases in either virtual or physical marketplaces; a single entity performs all of the required steps in authorizing a purchase (either in house if the customer is a customer of the host system, or sending out authorization to the customer's bank if the customer is not a customer of the host bank). The host system as a single entity as disclosed by O'Leary is able to perform each step of the transaction process.

Applicant argues the use of predetermined types of transaction and the validation of transactions based on making a determination of a predetermined type or not-predetermined type and the use of validation networks as claimed in O'Leary have not been clearly set forth by Examiner.

Per the present application, a predetermined transaction type means no credit card is being used and a non-predetermined type means a credit card is being used. O'Leary discloses in column 10, lines 17-21 where a determination is made as to whether electronic cash (no credit card) or credit card will be used for a transaction. O'Leary discloses determining whether the transaction is of a predetermined or non-predetermined type.

At this point, O'Leary discloses two validation networks by which authorization is obtained.

First, with regards to a predetermined transaction type, meaning no credit card. O'Leary discloses a "push" technology, conducted as follows: verifying the consumer has an account and then authorizing by a host bank and system operator (column 5, lines 51-60); if the transaction type is a predetermined type, a transfer is conducted through the host and EFT networks (column 7, lines 8-23) in order to conduct the transaction operation as disclosed by O'Leary (column 10, lines 21-35).

Second, with regards to a non-predetermined transaction type, meaning a credit card. O'Leary discloses a traditional "pull" technology, conducted as follows: verifying a consumer by contacting a credit card issuer for authorization if the transaction type is a non-predetermined type (column 5, lines 42-50; column 7, lines 3-7) in order to conduct the transaction operation as disclosed by O'Leary (column 10, lines 21-35).

O'Leary discloses two separate and distinct transaction types of a predetermined and non-predetermined type, and two techniques by which transactions are subsequently authorized based upon said determination. For predetermined transactions (virtual cash), the host system verifies the consumer using the central databases maintained by the host. For non-predetermined transactions (credit cards), the authorization is conducted by the card issuer.

Conclusion

Any inquiry concerning this communication should be directed to Jennifer Liversedge whose telephone number is 571-272-3167. The examiner can normally be reached on Monday – Friday, 8:30 – 5 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Sam Sough can be reached at 571-272-6799. The fax number for the organization where the application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jennifer Liversedge

Examiner

Art Unit 3628

HYUNG SOUGH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600